A proof for the oddity formula

Fabian Werner

Abstract

We show the so-called oddity formula for matrices/lattices. It states that for a symmetric, non.degenerate matrix $M \in \mathbb{Q}^{n\times n}$ the following relation holds:

$$\mathrm{sig}_{-1}(M) + \sum_{p\geq 3} p\text{-}\operatorname{excess}(M) \equiv \operatorname{oddity}(M) \mod 8$$

The necessary symbols like $\mathrm{sig}_{-1}(M), p\text{-}\operatorname{excess}(M), \operatorname{oddity}(M)$ will be defined in a precise manner. Some knowledge about the p-adic numbers is required.

Let K be a field, $R \subset K$ be a subring and $X, Y \in R^{n\times n}$. X and Y are called R-similar or R-equivalent, written $X \sim_R Y$ if there exists a matrix $V \in R^{n\times n}$ such that $V^{-1} \in R^{n\times n}$ and $Y = V^T X V$ where V^T is the transposed matrix. We put $\mathbb{P} := \{2, 3, 5, 7, 11, ...\}$ to be the set of prime numbers. Unless explicitly mentioned, p denotes a fixed prime number in $\mathbb{P}$.
We recall some basic facts about $\mathbf{Q_p}$ and $\mathbf{Z_p}$, the p-adic integers:

1 Theorem. *Let $\alpha \in \mathbf{Z_p}$ then there exists a uniquely determined sequence $(\alpha_n)_{n\in\mathbb{N}_0}$ such that $0 \leq \alpha_n \leq p-1$ such that*

$$\alpha = \sum_{n=0}^{\infty} \alpha_n p^n$$

where the sum on the right converges absolutely in the norm $|\cdot|_p$ on $\mathbf{Q_p}$. Further, for any $\beta \in \mathbf{Q_p}$ there are uniquely determined $N \in \mathbb{Z}$ and $(\beta_n)_{n\geq N}$ such that

$$\beta = \sum_{n\geq N} \beta_n p^n$$

where the sum on the right converges absolutely and $\sum_{n=0}^{\infty} beta_n p^n \in \mathbf{Z_p}$. Summarized, every p-adic integer may be written as a unique "power series" in p and every $\beta \in \mathbf{Q_p}$ may be written as a unique "Laurent series" in p. Further, $\beta \in \mathbf{Z_p}^\times \iff |\beta|_p = 1 \iff \beta_0 \neq 0$

2 Corollary. *In particular, it follows that either $\beta \in \mathbf{Z_p}$ (if $N \geq 0$) or if $N = -M$ then*

$$\beta = \frac{\beta{-}M}{p^M} + ... + \frac{\beta{-}1}{p^1} + \underbrace{\beta'}_{\in \mathbf{Z_p}} \in \frac{\beta{-}M + p\beta_{-M+1} + ... + p^{M-1}\beta_{-1}}{p^M} + \mathbf{Z_p}$$

so that $\mathrm{Quot}(\mathbf{Z_p})$ *is given by an isomorphic copy of* $\mathbf{Q_p}$ *which will we identify with each other henceforth.*

3 Theorem. *For every* $e \in \mathbb{N}_0, \alpha \in \mathbf{Z_p}$ *there exist* $z \in \mathbb{Z}, \gamma \in \mathbf{Z_p}$ *such that*

$$\alpha = z + p^e \beta$$

If α *possesses a* p*-adic expansion* $\alpha = \alpha_0 p^0 + \alpha_1 p^1 + \ldots$ *then* z *is precisely given by* $z = \alpha_0 p^0 + \alpha_1 p^1 + \ldots + \alpha_{e-1} p^{e-1}$. *Further,* e, β, γ *are uniquely determined if we additionally require that* $\beta \in \mathbf{Z_p}^{\times}$.

For defining the p-excess we will need the subsequent symbols:

4 Definition. *Let* $m \in \mathbb{N}, s \in \mathbf{Z_p}$ *and*

$$s = s_0 + s_1 p + s_2 p^2 + \ldots + s_m p^m + \widetilde{s} p^{m+1}$$

be its unique p*-adic expansion with* $\widetilde{s} = s_{m+1} + p s_{m+1} + \ldots \in \mathbf{Z_p}$. *We define*

$$R_{p^m}(s) := s_0 + s_1 p + \ldots + s_m p^m \in \mathbb{Z}$$

Using some computations in $\mathbf{Z_p}$ one can show the following:

5 Lemma. R_{p^m} *is additive and multiplicative in the sense that for* $s, t \in \mathbf{Z_p}$,

(a) $R_{p^m}(s+t) \equiv R_{p^m}(s) + R_{p^m}(t) \mod p^m$

(b) $R_{p^m}(st) \equiv R_{p^m}(s) R_{p^m}(t) \mod p^m$

so that $R_{p^m} : \mathbf{Z_p} \mapsto \mathbb{Z}_{p^m}$ *is a homomorphism of rings.*

6 Definition (Legendre-symbol)**.** *Let* $p \in \mathbb{P}, x \in \mathbb{Z}$ *such that* $(x, p) = 1$. *We define the Legendre-symbol to be*

$$\left(\frac{x}{p}\right) := \begin{cases} +1 & \text{if } \exists r \in \mathbb{Z}_p \text{ with } r^2 \equiv x \mod p \\ -1 & \text{otherwise} \end{cases}$$

For the Legendre symbol there are a few famous rules that are due to Gauss:

7 Theorem. *For primes* $p, q \in \mathbb{P}$ *with* $p \neq 2, q \neq 2$ *the following relation (usually called the law of quadratic reciprocity) holds:*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

Furthermore,

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}, \quad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

Proof. See, for example, [Ne], Theorem 8.6, p. 53 or any book on algebraic number theory. □

8 Definition (Legendre-Jacobi-symbol)**.** *Let $m, n \in \mathbb{Z}$ so that there are $p_1, ..., p_r \in \mathbb{P}$, $\epsilon, \delta \in \{+1, -1\}$ and $n_1, ..., n_r, m_1, ..., m_r \in \mathbb{N} \cup \{0\}$ such that*

$$n = \epsilon p_1^{n_1} \cdots p_r^{n_r}, \quad m = \delta p_1^{m_1} \cdots p_r^{m_r}$$

We define

$$\gcd(m, n) := (-1)^{\min(\epsilon,\delta)} p_1^{\min(n_1,m_1)} \cdots p_r^{\min(n_r,m_r)} = (-1)^{\min(\epsilon,\delta)} \gcd(|n|, |m|)$$

If $\gcd(n, m) = +1$ we define the Legendre-Jacobi Symbol to be

$$m = p \in \mathbb{P} \Rightarrow \left(\frac{n}{m}\right) := \left(\frac{n}{p}\right) (\textit{in the sense of Def. 6})$$

$$m = 2 \Rightarrow \left(\frac{n}{2}\right) := \begin{cases} +1 & \textit{if } n \equiv \pm 1 \mod 8 \\ -1 & \textit{otherwise} \end{cases}$$

$$m = -1 \Rightarrow \left(\frac{n}{-1}\right) := +1$$

$$m = \delta p_1^{m_1} \cdots p_r^{m_r} \Rightarrow \left(\frac{n}{m}\right) := \left(\frac{n}{-1}\right)^{\delta} \left(\frac{n}{p_1}\right)^{m_1} \cdots \left(\frac{n}{p_r}\right)^{m_r}$$

Further, for $s \in \mathbf{Z_p}$ we set

$$\left(\frac{s}{p}\right) := \begin{cases} \left(\frac{R_8(s)}{2}\right) & \textit{if } p = 2 \\ \\ \left(\frac{R_p(s)}{p}\right) & \textit{otherwise} \end{cases}$$

9 Definition. *Let $p \in \mathbb{P}$. Every $\alpha \in \mathbf{Q_p}$ can be uniquely written as $\alpha = p^{\nu}\beta$ with $|\beta|_p = 1$ and $\nu \in \mathbb{Z}$. We say that α is a p-adic antisquare if*

(i) ν *is odd*

(ii) $\left(\frac{\beta}{p}\right) = -1$

10 Notation. *We extend the set of "primes" to $\overline{P} = \{-1\} \cup \mathbb{P}$ and write $\mathbb{Q}_{-1} := \mathbb{R}$.*

11 Definition. *Let K be a field and $X \in K^{n\times n}$ be a symmetric non-degenerate matrix. From linear algebra (e.g. see [Fi], p.325) we know that we can find a matrix $V \in K^{n\times n}$, $\det(V) \in K^{\times}$ with $V^T XV = \mathrm{diag}(q_1, ..., q_n)$ for some $q_1, ..., q_n \in K$. If $X \in \mathbf{Q_p}$ then we define the so-called p-signature of X (with respect to V) as follows:*

(a) If $p = -1$ then $\mathbf{Q_p} = \mathbb{R}$ and by basic linear algebra we find $V \in \mathbb{R}^{n\times n}$ with $\det(V) \neq 0$ such that $V^T XV = \mathrm{diag}(\epsilon_1, ..., \epsilon_n)$ with $\epsilon_i \in \{\pm 1\}$. Let $l_- := |\{i \ : \ \epsilon_i = -1\}|$ and $l_+ := |\{i \ : \ \epsilon_i = +1\}|$ then

$$\mathrm{sig}_{-1}(X) := l_+ - l_- \mod 8$$

(b) Let $p \geq 2$. Seen as element in $\mathbf{Q_p}$, we may write $q_i = p^{\nu_i}\beta_i$ with $|\beta|_p = 1$. Set

$$m := |\{i \in \{1, ..., n\} \ : \ q_i \text{ is a } p\text{-adic antisquare}\}|$$

Let $x = \frac{a}{b} \in \mathbb{Q}$ such that $(b, p) = 1$ then we always put $x \mod 8 := a \cdot b^{-1} \mod 8$. It is easily checked that this map does not depend on the representative of q, i.e. if $q = \frac{c}{d}$, then $cd^{-1} \equiv ab^{-1} \mod 8$. In this sense we put

$$\mathrm{sig}_p(X) := \begin{cases} p^{\nu_1} + ... + p^{\nu_n} + 4m \mod 8 & \text{if } p > 2 \\ R_8(\beta_1) + ... + R_8(\beta_n) + 4m \mod 8 & \text{if } p = 2 \end{cases}$$

The 2-signature of X will also be called oddity of X. Furthermore we define

$$p\text{−}\mathrm{excess}(X) := \begin{cases} \mathrm{sig}_p(X) - n \mod 8 & \text{if } p \neq 2 \\ n - \mathrm{sig}_2(X) \mod 8 & \text{otherwise} \end{cases}$$

12 Remark. *Let $p \in \overline{P}$, then the p-signature is an invariance under different diagonalization processes (i.e. if V, W both diagonalize X in the sense of the above, then the p-signature of X with respect to the diagonalization of V is actually the same as the one with respect to the diagonalization of W) and furthermore it is an invariance under $\mathbf{Q_p}$-similarity, i.e. if $X \sim_{\mathbf{Q_p}} Y$ then* $\mathrm{sig}_p(X) \equiv \mathrm{sig}_p(Y) \mod 8$.

Proof. The result for $p = -1$ is called Sylvesters law of inertia. It is due to basic linear algebra. A proof can be found in [Fi], p. 323 or any undergraduate textbook on linear algebra. For $p \neq -1$, the proof is written down in [CS], chapter 15, §6. 6.1. and the first half of 6.2. □

13 Notation. *For two matrices $A \in K^{n\times n}, B \in K^{m\times m}$ we denote by $A \oplus B$ the $(n+m)\times(n+m)$ matrix*

$$A \oplus B := \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$$

It is easy to see that $\mathrm{sig}_p(A \oplus B) = \mathrm{sig}_p(A) + \mathrm{sig}_p(B)$ for all $p \in \overline{\mathbb{P}}$.
Now we know all the symbols that occur in the oddity formula. For the proof we need once more new symbols called the Hilbert norm residue symbol.

14 Definition. *Let $p \in \mathbb{P}$ and $a, b \in \mathbf{Q_p}^\times$. We put*

$$\left(\frac{a,b}{p}\right) := \begin{cases} +1 & \textit{if } \mathrm{diag}(a,b,-1) \textit{ is non-trivially isotropic} \\ -1 & \textit{otherwise} \end{cases}$$

Where some matrix $M \in \mathbf{Q_p}^{n\times n}$ is called non-trivially isotropic if there exists a non-trivial isotropic vector, that is a vector $x = (x_1, ..., x_n) \in \mathbf{Q_p}^n \setminus \{(0, ..., 0)\}$ such that $xMx^T = 0$.

So the above symbol is defined as

$$\left(\frac{a,b}{p}\right) := \begin{cases} +1 & \text{if } \exists (x,y,z) \in \mathbf{Q_p}^3 \setminus \{(0,0,0)\} \text{ such that } ax^2 + by^2 - z^2 = 0 \\ -1 & \text{otherwise} \end{cases}$$

Occasionally we will write (a, b) in place for $(\frac{a,b}{p})$ whenever the prime p is clear from the context. The following rules apply:

15 Lemma. *For the Hilbert norm residue symbol for a fixed prime p and $a, b, c \in \mathbf{Q_p}^\times$ we have*

- $(a, b) = (b, a)$
- $(ab, c) = (a, c)(b, c)$
- $(a, bc) = (a, b)(a, c)$

Proof. See [Ca], Lemma 2.1 on page 42. □

For that reason (and because of $(a,b)^2 = (\pm 1)^2 = +1$), it suffices to know the values of the Hilbert symbol on a set of representatives of the quotient of abelian groups $Q(p) := \mathbf{Q_p}^\times/(\mathbf{Q_p}^\times)^2$. In order to understand the relation of this symbol to the p-excesses we need to know more about this group (or, respcetively, about squares in $\mathbf{Q_p}$). Let $v \in \mathbb{Z}, n \in \mathbb{N}$ then there exists a unique minimal positive representative of $v \mod n$, i.e. a unique number $v' \in \mathbb{Z}$ such that $v' \equiv v \mod n$ and $0 \leq v' \leq (n-1)$. We put $v \,\mathrm{modd}\, n := v' \in \mathbb{N}$.

16 Theorem. *Let $p \in \mathbb{P}, p \neq 2$. Chose $r \in \mathbb{Z}$ such that $(r,p) = 1$ and $(\frac{r}{p}) = 1$ (i.e. r is not a square in $\mathbb{Z}_p$). The group $Q(p) := \mathbf{Q_p}^\times/(\mathbf{Q_p}^\times)^2$ is of order 4 and it is given by*

$$Q(p) = \{1 \cdot (\mathbf{Q_p}^\times)^2, r \cdot (\mathbf{Q_p}^\times)^2, p \cdot (\mathbf{Q_p}^\times)^2, rp \cdot (\mathbf{Q_p}^\times)^2\}$$

The multiplication is given by

$$(r^x p^y \cdot (\mathbf{Q_p}^\times)^2) \cdot (r^z p^w \cdot (\mathbf{Q_p}^\times)^2) = r^{x+z \operatorname{modd} 2} p^{y+w \operatorname{modd} 2} \cdot (\mathbf{Q_p}^\times)^2$$

If $p = 2$ then the group $Q(p) := \mathbf{Q_p}^\times/(\mathbf{Q_p}^\times)^2$ is of order 8 and it is given by

$$Q(p) = \{(-1)^x 2^y 5^z \cdot (\mathbf{Q_p}^\times)^2 \mid x, y, z \in \{0,1\}\}$$

The multiplication is given by

$$((-1)^x 2^y 5^z \cdot (\mathbf{Q_p}^\times)^2) \cdot ((-1)^{x'} 2^{y'} 5^{z'} \cdot (\mathbf{Q_p}^\times)^2) = (-1)^{x+x' \operatorname{modd} 2} 2^{y+y' \operatorname{modd} 2} 5^{z+z' \operatorname{modd} 2} \cdot (\mathbf{Q_p}^\times)^2$$

Proof. See [Ca], corollary on page 40. □

Remark that for $p \geq 3$ we can always find such an r: By basic algebra, the group $\mathbb{Z}_p^\times$ is cyclic (as its is the multiplicative group of the finite field $\mathbb{F}_p$), let g be its generator. The squares in $\mathbb{Z}_p^\times$ are precisely given by g^x where $0 \leq x \leq \operatorname{ord}(g)$ and x is even. Hence, we may select one of the elements $g, g^3, g^5, ...$ as r.

The Hilbert norm residue symbol is important because it gives rise to the so-called Hasse-Minkowski invariant:

17 Definition. *Let $X \in \mathbf{Q_p}^{n \times n}$ be an invertible, symmetric matrix. By basic linear algebra, $X \sim_{\mathbf{Q_p}} \operatorname{diag}(a_1, ..., a_n)$ for some matrix $V \in \mathbf{Q_p}^{n \times n}$ with $\det(V) \neq 0$. We define the Hasse-Minkowski symbol for X with respect to V to be*

$$c_p(X) := \prod_{1 \leq i < j \leq n} \left(\frac{a_i, a_j}{p} \right)$$

18 Remark. *$c_p(X)$ does actually not depend on V and if $X \sim_{\mathbf{Q_p}} Y$, then $c_p(X) = c_p(Y)$. For this reason, $c_p(X)$ is called the Hasse-Minkowski invariant.*

Proof. See [Ca], chapter 4, sections 1 and 2. □

We introduce one last new symbol, the so-called p-signature-symbol:

19 Definition. *Let $X \in \mathbf{Q_p}^{n\times n}$ be an invertible, symmetric matrix. By basic linear algebra, $X \sim_{\mathbf{Q_p}} \mathrm{diag}(a_1, ..., a_n)$ for some matrix $V \in \mathbf{Q_p}^{n\times n}$ with $\det(V) \neq 0$. We define the p-signature-symbol for X with respect to V to be*

$$p(X) := \begin{cases} +1 & \textit{if } \mathrm{sig}_p(\mathrm{diag}(a_1, ..., a_n)) \equiv \mathrm{sig}_p(\mathrm{diag}(a_1 \cdot ... \cdot a_n, 1, ..., 1)) \mod 8 \\ -1 & \textit{otherwise} \end{cases}$$

Now we prepare the proof for the oddity formula. Here we prove that the Hasse-Minkowski symbol and the p-signature-symbol actually coincide.

20 Theorem. *For every $X \in \mathbf{Q_p}^{n\times n}$, we have*

$$p(X) = c_p(X)$$

hence, the p-signature-symbol does not depend on the diagonalization process and it is an invariant. Furthermore, if $\mathrm{sig}_p(\mathrm{diag}(a_1, ..., a_n)) \not\equiv \mathrm{sig}_p(\mathrm{diag}(a_1 \cdot ... \cdot a_n, 1, ..., 1)) \mod 8$ then both expressions differ by $4 \mod 8$.

Proof. We proceed by induction on n. Let $n = 2$. We first compute the values of the p-signature symbol on certain special elements, namely the representatives of $Q(p)$: Let $p \in \mathbb{P}, p \geq 3$ and let further $A = p^x\alpha, B = p^y\beta$ with $\alpha, \beta \in \{1, r\}$. Put

$$(p \equiv x) := \begin{cases} +1 & \text{if } p \equiv x \mod 4 \\ -1 & \text{otherwise} \end{cases}$$

then we have the following table:

A	B	x	y	$(\frac{\alpha}{p})$	$(\frac{\beta}{p})$	$4k$	$4k'$	$\mathrm{sig}_p(\begin{smallmatrix} A & 0 \\ 0 & B \end{smallmatrix})$	$\mathrm{sig}_p(\begin{smallmatrix} AB & 0 \\ 0 & 1 \end{smallmatrix})$	$p(\begin{smallmatrix} A & 0 \\ 0 & B \end{smallmatrix})$
r	r	0	0	-1	-1	0	0	2	$1+1$	$+1$
r	1	0	0	-1	$+1$	0	0	2	$1+1$	$+1$
1	r	0	0	$+1$	-1	0	0	2	$1+1$	$+1$
1	1	0	0	$+1$	$+1$	0	0	2	$1+1$	$+1$
r	pr	0	1	-1	-1	4	0	$1+p+4$	$1+p$	-1
r	p	0	1	-1	$+1$	0	4	$1+p$	$1+p+4$	-1
1	pr	0	1	$+1$	-1	4	4	$1+p+4$	$1+p+4$	$+1$
1	p	0	1	$+1$	$+1$	0	0	$1+p$	$1+p$	$+1$
pr	r	1	0	-1	-1	4	0	$1+p+4$	$1+p$	-1
pr	1	1	0	-1	$+1$	4	4	$1+p+4$	$1+p+4$	$+1$
p	r	1	0	$+1$	-1	0	4	$1+p$	$1+p+4$	-1
p	1	1	0	$+1$	$+1$	0	0	$1+p$	$1+p$	$+1$
pr	pr	1	1	-1	-1	0	0	$2p$	$1+1$	$(p \equiv 1)$
pr	p	1	1	-1	$+1$	4	0	$2p+4$	$1+1$	$(p \equiv 3)$
p	pr	1	1	$+1$	-1	4	0	$2p+4$	$1+1$	$(p \equiv 3)$
p	p	1	1	$+1$	$+1$	0	0	$2p$	$1+1$	$(p \equiv 1)$

Remarks concrning the last four lines: Consider the case $A = pr = B$, then

$$\begin{aligned} p(\begin{smallmatrix} A & 0 \\ 0 & B \end{smallmatrix}) = +1 &\iff 2p \equiv 2 \mod 8 \iff \exists v \in \mathbb{Z} \;\; 2p - 2 = 8v \\ &\iff \exists v \in \mathbb{Z} \;\; p - 1 = 4v \iff p \equiv 1 \mod 4 \end{aligned}$$

and analogously we verify the last three lines. We also remark that in the first 12 cases, it is clear that if the p-siganture are different then they vary by $4 \mod 8$. Concerning this assertion in the last four cases: Consider the case $A = pr = B$ and assume that the signature do not coincide (i.e. $p \equiv 3 \mod 4$ as shown above) so that there exists a $v \in \mathbb{Z}$ such that $p = 4v + 3$. We compute

$$\mathrm{sig}_p(\begin{smallmatrix} A & 0 \\ 0 & B \end{smallmatrix}) - \mathrm{sig}_p(\begin{smallmatrix} AB & 0 \\ 0 & 1 \end{smallmatrix}) \equiv 2p - 2 \equiv 2(4v+3) - 2 \equiv 8v + 6 - 2 \equiv 4 \mod 8$$

and analogously we verify the remaining three cases so that we have shown the second half of the assertion for the case $n = 2, p \geq 3$. Let us prove the first half of the theorem in this case. We rearrange the table to a more compact form; now each cell just contains the result $p\left(\begin{smallmatrix} A & 0 \\ 0 & B \end{smallmatrix}\right)$:

$B \backslash A$	1	r	p	rp
1	$+1$	$+1$	$+1$	$+1$
r	$+1$	$+1$	-1	-1
p	$+1$	-1	$p \equiv 1$	$p \equiv 3$
rp	$+1$	-1	$p \equiv 1$	$p \equiv 3$

If we compare this table to the one given in [Ca] in the proof of Lemma 2.1, p. 43 that summarizes the results of $(\frac{A,B}{p})$ (remark that Cassels uses the symbol ϵ instead of $(p \equiv 1)$, then $-\epsilon = (p \equiv 3)$) we see that the numbers $p\left(\begin{smallmatrix} A & 0 \\ 0 & B \end{smallmatrix}\right)$ and $(\frac{A,B}{p})$ coincide.

Now let $a, b \in \mathbf{Q_p}^\times$, then by Thm. 16, there are $v, w \in \mathbf{Q_p}^\times$ such that $a = v^2 A, b = w^2 B$ for $A, B \in \{1, r, p, pr\}$. We then have

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} = \begin{pmatrix} v & 0 \\ 0 & w \end{pmatrix} \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} \begin{pmatrix} v & 0 \\ 0 & w \end{pmatrix}$$

hence, $\left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right) \sim_{\mathbf{Q_p}} \left(\begin{smallmatrix} A & 0 \\ 0 & B \end{smallmatrix}\right)$. All in all we obtain

$$\begin{aligned} \left(\frac{a,b}{p}\right) &= \underbrace{\left(\frac{v,b}{p}\right)^2}_{=(\pm 1)^2 = +1} \left(\frac{A,B}{p}\right) \underbrace{\left(\frac{a,w}{p}\right)^2}_{=(\pm 1)^2 = +1} && \text{(by Lemma 15)} \\ &= p\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} && \text{(by the above)} \\ &= p\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \\ & \qquad \text{(as the } p\text{-signature is invariant under } \sim_{\mathbf{Q_p}}) \end{aligned}$$

We have shown the theorem for the case $n = 2, p \geq 3$ and the cases $n = 2, p \in \{-1, 2\}$ work out in a completely analogous way (setup a table for the p-signatures as above, verify for each line that the p-signatures may only vary by $4 \mod 8$ provided that they are unequal and then compare the table with the results of $p(\cdot)$ to the respective table in [Ca] on page 43 and 44). Now we proceed to higher dimensions. Assume that $c_p(X) = +1$. For $i \in \{1, ..., n\}$ put $A_i := (\frac{a_i, a_1 \cdot ... \cdot a_{i-1} \cdot a_{i+1} \cdot ... \cdot a_n}{p})$. Let us assume that there exists an A_i with $A_i = +1$, then since $c_p(\cdot)$ is an invariant under $\mathbf{Q_p}$-similarity we may switch the positions of a_i and a_1 so that we may assume $A_1 = +1$. Now

$$\begin{aligned} 1 = c_p(X) &= \prod_{1 \leq i < j \leq n} \left(\frac{a_i, a_j}{p}\right) \\ &= \prod_{1 \leq i \leq n} \left(\frac{a_i, a_{i+1} \cdot ... \cdot a_n}{p}\right) && \text{(by Lemma 15)} \\ &= \underbrace{A_1}_{=+1} \cdot \prod_{2 \leq i \leq n} \left(\frac{a_i, a_{i+1} \cdot ... \cdot a_n}{p}\right) \\ &= c_p(\mathrm{diag}(a_2, ..., a_n)) \end{aligned}$$

Therefore, by the induction hypothesis

$$\operatorname{sig}_p(\operatorname{diag}(a_2, ..., a_n)) \equiv \operatorname{sig}_p(\operatorname{diag}(a_2 \cdot ... \cdot a_n, 1, ..., 1)) \mod 8 \qquad (0.1)$$

We obtain

$$\begin{aligned}\operatorname{sig}_p(\operatorname{diag}(a_1, ..., a_n)) &\equiv \operatorname{sig}_p((a_1)) + \operatorname{sig}_p(\operatorname{diag}(a_2, ..., a_n))\\ &\equiv \operatorname{sig}_p((a_1)) + \operatorname{sig}_p(\operatorname{diag}(a_2 \cdot ... \cdot a_n, 1, ..., 1)) && \text{(by (0.1))}\\ &\equiv \operatorname{sig}_p\begin{pmatrix} a_1 & 0 \\ 0 & a_2 \cdot ... \cdot a_n \end{pmatrix} + \operatorname{sig}_p(\operatorname{diag}(1, ..., 1))\\ &\equiv \operatorname{sig}_p\begin{pmatrix} a_1 \cdot a_2 \cdot ... \cdot a_n & 0 \\ 0 & 1 \end{pmatrix} + \operatorname{sig}_p(\operatorname{diag}(1, ..., 1)) && \text{(as } A_1 = +1)\\ &\equiv \operatorname{sig}_p(\operatorname{diag}(a_1 ... a_n, 1, ..., 1))\end{aligned}$$

(0.2)

Now assume $c_p(X) = +1$ but $A_i = -1$ for all i, in particular $A_1 = -1$ so that by the same argument as above,

$$1 = c_p(X) = A_1 c_p(\operatorname{diag}(a_2, ..., a_n)) = -c_p(\operatorname{diag}(a_2, ..., a_n))$$

i.e., by the induction hypothesis,

$$\operatorname{sig}_p(\operatorname{diag}(a_2, ..., a_n)) \equiv \operatorname{sig}_p(\operatorname{diag}(a_2 \cdot ... \cdot a_n, 1, ..., 1)) + 4 \mod 8 \qquad (0.3)$$

Also note that using $A_1 = -1$ and the correctness of the assertion in the case $n = 2$, we obtain

$$\operatorname{sig}_p\begin{pmatrix} a_1 & 0 \\ 0 & a_2 \cdot ... \cdot a_n \end{pmatrix} \equiv \operatorname{sig}_p\begin{pmatrix} a_1 \cdot a_2 \cdot ... \cdot a_n & 0 \\ 0 & 1 \end{pmatrix} + 4 \mod 8 \qquad (0.4)$$

so that

$$\begin{aligned}\operatorname{sig}_p(\operatorname{diag}(a_1, ..., a_n)) &\equiv \operatorname{sig}_p((a_1)) + \operatorname{sig}_p(\operatorname{diag}(a_2, ..., a_n))\\ &\equiv \operatorname{sig}_p((a_1)) + \operatorname{sig}_p(\operatorname{diag}(a_2 \cdot ... \cdot a_n, 1, ..., 1)) + 4 && \text{(by (0.3))}\\ &\equiv \operatorname{sig}_p\begin{pmatrix} a_1 & 0 \\ 0 & a_2 \cdot ... \cdot a_n \end{pmatrix} + \operatorname{sig}_p(\operatorname{diag}(1, ..., 1)) + 4\\ &\equiv \operatorname{sig}_p\begin{pmatrix} a_1 \cdot a_2 \cdot ... \cdot a_n & 0 \\ 0 & 1 \end{pmatrix} + 4 + \operatorname{sig}_p(\operatorname{diag}(1, ..., 1)) + 4 && \text{(by (0.4))}\\ &\equiv \operatorname{sig}_p(\operatorname{diag}(a_1 ... a_n, 1, ..., 1)) + 8\\ &\equiv \operatorname{sig}_p(\operatorname{diag}(a_1 ... a_n, 1, ..., 1)) \mod 8\end{aligned}$$

If we assume that $c_p(X) = -1$ then we do the same computation as in (0.1) to obtain that either $A_1 = -1$ and $c_p(\text{diag}(a_2, ..., a_n)) = +1$ or vice versa. In the first case we obtain

$$\begin{aligned}
\text{sig}_p(\text{diag}(a_1, ..., a_n)) &\equiv \text{sig}_p((a_1)) + \text{sig}_p(\text{diag}(a_2, ..., a_n)) \\
&\equiv \text{sig}_p((a_1)) + \text{sig}_p(\text{diag}(a_2 \cdot ... \cdot a_n, 1, ..., 1)) && \text{(by (0.1))} \\
&\equiv \text{sig}_p \begin{pmatrix} a_1 & 0 \\ 0 & a_2 \cdot ... \cdot a_n \end{pmatrix} + \text{sig}_p(\text{diag}(1, ..., 1)) \\
&\equiv \text{sig}_p \begin{pmatrix} a_1 \cdot a_2 \cdot ... \cdot a_n & 0 \\ 0 & 1 \end{pmatrix} + 4 + \text{sig}_p(\text{diag}(1, ..., 1)) + 4 && \text{(by (0.4))} \\
&\equiv \text{sig}_p(\text{diag}(a_1 ... a_n, 1, ..., 1)) + 4
\end{aligned}$$

and in the latter one, the "error" in the second line disappears but precisely one new "error" occurs in line 4. Thus

$$\text{sig}_p(\text{diag}(a_1, ..., a_n)) \equiv \text{sig}_p(\text{diag}(a_1 ... a_n, 1, ..., 1)) + 4 \mod 8$$

□

The above insight allows a fundamental simplification of the assertion that we have to prove in order to prove the oddity formula. First we need a fact about the $c_p(\cdot)$:

21 Theorem. *For a non-degenerate, symmetric matrix $X \in \mathbb{Q}^{n \times n}$, $c_p(X) = -1$ can only occur for finitely many $p \in \overline{\mathbb{P}}$ and furthermore*

$$\prod_{p \in \overline{\mathbb{P}}} c_p(X) = +1$$

i.e. $c_p(X) = -1$ occurs only for an even number of primes $p \in \overline{\mathbb{P}}$.

Proof. See [Ca], Lemma 3.4, p. 46. □

Let $X \in \mathbb{Q}^{n \times n}$ be a symmetric, non-degenerate matrix with $X \sim_{\mathbf{Q_p}} \text{diag}(a_1, ..., a_n)$. Put $Y := \text{diag}(a_1 ... a_n, 1, ..., 1)$. Firstly, we observe that the oddity formula is obviously equivalent to

$$\sum_{p \in \overline{\mathbb{P}}} p\text{– excess}(X) \equiv 0 \mod 8$$

We compare the expression to $\sum_{p\in\overline{\mathbb{P}}} p\text{–}\operatorname{excess}(Y)$. Let $Q := \{p_1, ..., p_{2k}\}$ be those prime numbers for which $c_p(X) = -1$, then by Thm. 20,

$$\operatorname{sig}_{p_j}(X) \equiv \operatorname{sig}_{p_j}(\operatorname{diag}(a_1...a_n, 1, ..., 1)) + 4 \mod 8$$

or rather

$$p_j\text{–}\operatorname{excess}(X) \equiv p_j\text{–}\operatorname{excess}(\operatorname{diag}(a_1...a_n, 1, ..., 1)){+}4 = p_j\text{–}\operatorname{excess}(Y){+}4 \mod 8$$

and furthermore, for all $p \notin Q$,

$$p\text{–}\operatorname{excess}(X) \equiv p\text{–}\operatorname{excess}(\operatorname{diag}(a_1...a_n, 1, ..., 1)) = p\text{–}\operatorname{excess}(Y) \mod 8$$

so that

$$\begin{aligned}\sum_{p\in\overline{\mathbb{P}}} p\text{–}\operatorname{excess}(X) &\equiv \sum_{j=1}^{2k} p_j\text{–}\operatorname{excess}(X) + \sum_{p\notin Q} p\text{–}\operatorname{excess}(X)\\ &\equiv \sum_{j=1}^{2k}(p_j\text{–}\operatorname{excess}(Y) + 4) + \sum_{p\notin Q} p\text{–}\operatorname{excess}(Y)\\ &\equiv \sum_{p\in\overline{\mathbb{P}}} p\text{–}\operatorname{excess}(Y) + 2k\cdot 4\\ &\equiv \sum_{p\in\overline{\mathbb{P}}} p\text{–}\operatorname{excess}(Y) \mod 8\end{aligned} \tag{0.5}$$

Consequently, it suffices to show that for every number $a \in \mathbb{Q}^\times$

$$\sum_{p\in\overline{\mathbb{P}}} p\text{–}\operatorname{excess}(Y) \equiv 0 \mod 8$$

for $Y = \operatorname{diag}(a, 1, ..., 1)$ and this is what we will do now.

22 Theorem. *Let $a \in \mathbb{Q}^\times$, let $m \in \mathbb{N}$ and put $Y' := \operatorname{diag}(\underbrace{1, ..., 1}_{(m-1)\ times})$ then, for the matrix $Y := (a) \oplus Y' \in \mathbb{Q}^{m\times m}$ we have*

$$\sum_{p\in\overline{\mathbb{P}}} p\text{–}\operatorname{excess}(Y) \equiv 0 \mod 8$$

Proof. Let $a = (-1)^x 2^y p_1^{x_1} \cdot ... \cdot p_n^{x_n}$ for $x \in \{0,1\}, y \in \mathbb{Z}$ and $x_i \in \mathbb{Z}$ for some odd primes $p_1, ..., p_n \in \mathbb{P} \setminus \{2\}$. Write $y = 2k + r$ with $k \in \mathbb{Z}, 0 \leq r \leq 1$, then

$$\operatorname{diag}(a, 1, ..., 1) = \operatorname{diag}(2^k, 1, ..., 1) \operatorname{diag}((-1)^x 2^r p_1^{x_1} \cdot ... \cdot p_n^{x_n}) \operatorname{diag}(2^k, 1, ..., 1)$$

Since the p-signatures (and therefore the p-excesses) are invariants under $\sim_{\mathbf{Q_p}}$, the p-excess of Y and the one of $\operatorname{diag}((-1)^x 2^r p_1^{x_1} \cdot ... \cdot p_n^{x_n})$ coincide (modulo 8). If we proceed analogously with the rest of the exponents, we may kill all squares and therefore assume henceforth that not only $x_i, y \in \mathbb{Z}$ but $x_i = 1$ (if some x_i is even then we simply leave out this prime number and resort the rest of them) and $y \in \{0,1\}$. Put

$$Q := \{p_1, ..., p_n\}$$

$$\delta : \{+1, -1\} \mapsto \mathbb{Z}_8, \quad \delta(+1) \equiv 0, \delta(-1) \equiv 1,$$

$$\Delta_2 := \begin{cases} 0 & \text{if y = 0} \\ \delta(\frac{(-1)^x p_1 ... p_n}{2}) & \text{otherwise} \end{cases}$$

and

$$\Delta_{\setminus p_j} := \delta\left(\frac{(-1)^x p_1 ... p_{j-1} p_{j+1} ... p_n}{p_j}\right)$$

At first we are going to assume that $x = 0$, i.e. a is positive. By definition of the p-excess,

- -1– excess$(Y) \equiv m - m \equiv 0$
- 2– excess$(Y) \equiv m - [p_1 ... p_n + (m-1) + 4\Delta_2] \equiv -(p_1 ... p_n) + 1 - 4\Delta_2$
- p_j– excess$(Y) \equiv p_j + (m-1) + \Delta_{\setminus p_j} - m \equiv p_j - 1 + \Delta_{\setminus p_j}$
- p– excess$(Y) \equiv m - m \equiv 0$ for all $p \notin Q$

Hence,

$$\sum_{p \in \overline{\mathbb{P}}} p\text{– excess}(Y) \equiv -(p_1 ... p_n) + 1 - 4\Delta_2 + \sum_{j=1}^{n} (p_j + 4\Delta_{\setminus p_j}) - n$$

Observe that the dimension of the matrix becomes completely irrelevant. We have to show that this sum is congruent to 0 modulo 8 and since $-4 \equiv +4$ mod 8, this is equivalent to saying that

$$4\Delta_2 + \sum_{j=1}^{n} 4\Delta_{\setminus p_j} \equiv 1 - (p_1 ... p_n) + \sum_{j=1}^{n} p_j - n \tag{0.6}$$

We will show this equation by induction on n.

We need two small preparations: Going through all the four cases for $x, y \in \{+1, -1\}$ yields

$$4\delta(xy) \equiv 4\delta(x) + 4\delta(y) \mod 8 \tag{0.7}$$

Moreover we will need the following Lemma

23 Lemma. *Let $x_1, ..., x_{n-1} \in \mathbb{Z}$ be odd numbers, then*

$$(x_1 - 1) + (x_2 - 1) + ... + (x_{n-1} - 1) \equiv x_1 ... x_{n-1} - 1 \mod 4$$

Proof. Since the x_i are odd, x_i is either congruent to 1 or 3 modulo 4. Resort the x_i so that $x_j - 1 \equiv 2 \mod 4$ for $1 \leq j \leq k$ and $x_j - 1 \equiv 0 \mod 4$ for $k + 1 \leq j \leq n - 1$. The left hand side evaluates to

$$\underbrace{(x_1 - 1)}_{\equiv 2 \mod 4} + ... + \underbrace{(x_k - 1)}_{\equiv 2 \mod 4} + \underbrace{(x_{k+1} - 1)}_{\equiv 0 \mod 4} + ... + \underbrace{(x_{n-1} - 1)}_{\equiv 0 \mod 4} \equiv 2r \mod 4$$

which is 2 iff. r is odd and 0 otherwise. Let us evaluate the right hand side:

$$\underbrace{x_1}_{\equiv -1} ... \underbrace{x_k}_{\equiv -1} \underbrace{x_{k+1}}_{\equiv 1} ... \underbrace{x_{n-1}}_{\equiv 1} - 1 \equiv (-1)^r - 1$$

and this in turn is precisely congruent to 2 iff. r is odd and it is congruent to 0 otherwise (and this coincides with the left hand side as computed above!). □

Now we will prove equation (0.6). The proof for $n = 1$ is a straightforward computation. Firstly, we will assume that $y = 0$, i.e. a is odd and $\Delta_2 = 0$. For increasing readability, we will use (0.7) without notification now in the induction step:

$$\begin{aligned}
\sum_{j=1}^{n} 4\Delta_{\backslash p_j} &\equiv \sum_{j=1}^{n-1} 4\delta\left(\frac{p_1 ... p_{j-1}p_{j+1}...p_{n-1}p_n}{p_j}\right) + 4\delta\left(\frac{p_1...p_{n-1}}{p_n}\right)\\
&\equiv \sum_{j=1}^{n-1} 4\delta\left(\frac{p_1 ... p_{j-1}p_{j+1}...p_{n-1}}{p_j}\right) + \sum_{j=1}^{n-1} 4\delta\left(\frac{p_n}{p_j}\right) + 4\delta\left(\frac{p_1...p_{n-1}}{p_n}\right)\\
&\overset{\text{ind. hyp.}}{\equiv} 1 - p_1...p_{n-1} + \sum_{j=1}^{n-1} p_j - (n-1) + \sum_{j=1}^{n-1} 4\delta\left(\frac{p_n}{p_j}\right) + 4\delta\left(\frac{p_1...p_{n-1}}{p_n}\right)\\
&\equiv 1 - p_1...p_n + \sum_{j=1}^{n} p_j - n - p_1...p_{n-1} + p_1...p_n - p_n + 1\\
&\qquad + \sum_{j=1}^{n-1} 4\delta\left(\frac{p_n}{p_j}\right) + 4\delta\left(\frac{p_1...p_{n-1}}{p_n}\right)\\
&\equiv 1 - p_1...p_n + \sum_{j=1}^{n} p_j - n + (p_1...p_{n-1})(p_n - 1) - (p_n - 1)\\
&\qquad + \sum_{j=1}^{n-1} 4\delta\left(\frac{p_n}{p_j}\right) + 4\delta\left(\frac{p_1...p_{n-1}}{p_n}\right)\\
&\equiv \underbrace{1 - p_1...p_n + \sum_{j=1}^{n} p_j - n}_{=\text{r.h.s!}}\\
&\qquad + (p_n - 1)[p_1...p_{n-1} - 1] + \sum_{j=1}^{n-1} 4\delta\left(\frac{p_n}{p_j}\right) + 4\delta\left(\frac{p_1...p_{n-1}}{p_n}\right)
\end{aligned}$$

Put

$$z := (p_n - 1)[p_1...p_{n-1} - 1] + \sum_{j=1}^{n-1} 4\delta\left(\frac{p_n}{p_j}\right) + 4\delta\left(\frac{p-1...p_{n-1}}{p_n}\right) \mod 8$$

then it suffices to show that $z \equiv 0 \mod 8$. We rewrite z using the law of quadratic reciprocity (cf. Thm. 7):

$$\begin{aligned}
z &\equiv (p_n-1)[p_1...p_{n-1}-1] + \sum_{j=1}^{n-1} 4\delta\left(\frac{p_n}{p_j}\right) + 4\delta\left(\frac{p_1...p_{n-1}}{p_n}\right) \\
&\equiv (p_n-1)[p_1...p_{n-1}-1] + \sum_{j=1}^{n-1} 4\delta\left(\left(\frac{p_j}{p_n}\right)(-1)^{\frac{p_n-1}{4}(p_j-1)}\right) + 4\delta\left(\frac{p_1...p_{n-1}}{p_n}\right) \\
&\equiv (p_n-1)[p_1...p_{n-1}-1] + 4\delta\left(\prod_{j=1}^{n-1}\left(\frac{p_j}{p_n}\right)\right) + 4\delta\left(\frac{p_1...p_{n-1}}{p_n}\right) + 4\delta\left(\prod_{j=1}^{n-1}(-1)^{\frac{p_n-1}{4}(p_j-1)}\right) \\
&\equiv (p_n-1)[p_1...p_{n-1}-1] + \cancel{8\cdot\delta\left(\frac{p_1...p_{n-1}}{p_n}\right)} + 4\delta\left((-1)^{\frac{p_n-1}{4}[(p_1-1)+...+(p_{n-1}-1)]}\right)
\end{aligned} \tag{0.8}$$

Lemma 23 implies that there is a $k \in \mathbb{Z}$ such that

$$[(p_1-1)+...+(p_{n-1}-1)] - [p_1...p_{n-1}-1] = 4k$$

and since (p_n-1) is even, $\frac{p_n-1}{2} \in \mathbb{Z}$ so that

$$(p_n-1)[(p_1-1)+...+(p_{n-1}-1)] - (p_n-1)[p_1...p_{n-1}-1] = 8\frac{p_n-1}{2}k$$

so that

$$(p_n-1)[(p_1-1)+...+(p_{n-1}-1)] \equiv (p_n-1)[p_1...p_{n-1}-1] \mod 8 \tag{0.9}$$

Now

$$\begin{aligned}
&4\delta\left((-1)^{\frac{p_n-1}{4}[(p_1-1)+...+(p_{n-1}-1)]}\right) \equiv 4 \iff \delta\left((-1)^{\frac{p_n-1}{4}[(p_1-1)+...+(p_{n-1}-1)]}\right) = 1 \\
&\iff (-1)^{\frac{p_n-1}{4}[(p_1-1)+...+(p_{n-1}-1)]} = -1 \\
&\iff \frac{p_n-1}{4}[(p_1-1)+...+(p_{n-1}-1)] \text{ is odd} \\
&\iff \exists k \in \mathbb{Z} \;\; \frac{p_n-1}{4}[(p_1-1)+...+(p_{n-1}-1)] = 2k+1 \\
&\iff \exists k \in \mathbb{Z} \;\; (p_n-1)[(p_1-1)+...+(p_{n-1}-1)] = 8k+4 \\
&\iff (p_n-1)[(p_1-1)+...+(p_{n-1}-1)] \equiv 4 \mod 8 \\
&\overset{(0.9)}{\iff} (p_n-1)[p_1...p_{n-1}-1] \equiv 4 \mod 8
\end{aligned} \tag{0.10}$$

i.e. in the case where the δ-term is 4 mod 8,

$$z \equiv (p_n-1)[p_1 ... p_{n-1}-1]+4\delta\left((-1)^{\frac{p_n-1}{4}[(p_1-1)+...+(p_{n-1}-1)]}\right) \equiv 4+4 \equiv 0 \mod 8$$

The same computation as in (0.10) shows that the δ term is $0 \mod 8$ if and only if $(p_n-1)[p_1 ... p_{n-1}-1] \equiv 0 \mod 8$ so that in this case,

$$z \equiv 0+0 \equiv 0 \mod 8$$

this concludes the induction step for a being an odd positive natural number. Remark that we have shown in particular that (use $z \equiv 0$ and $-4 \equiv 4 \mod 8$!)

$$(p_n-1)[p_1 ... p_{n-1}-1] \equiv 4\delta\left((-1)^{\frac{p_n-1}{4}[(p_1-1)+...+(p_{n-1}-1)]}\right) \tag{0.11}$$

which will be used later in the case where a is negative. Now let a be positive (i.e. $x=0$) and even (i.e. $y=1$), then a very similar computation as above in the induction step shows that

$$4\Delta_2 + \sum_{j=1}^{n} 4\Delta_{\backslash p_j} \equiv 1-(p_1 ... p_n)+\sum_{j=1}^{n} p_j - n + z'$$

where $z' \equiv z + 4\delta\left(\frac{p_n}{2}\right) + 4\delta\left(\frac{2}{p_n}\right) \mod 8$. Since we have already shown that $z \equiv 0 \mod 8$, it suffices to show now that $z'' := 4\delta\left(\left(\frac{p_n}{2}\right)\left(\frac{2}{p_n}\right)\right) \equiv 0 \mod 8$: 1st case: $p_n = 8k \pm 1$, then

$$\frac{p_n^2-1}{8} = \frac{8^2k^2 \pm 2 \cdot 8 \cdot k + 1 - 1}{8} = 2[4k^2 \pm k]$$

is even so that by Thm. 7, $(\frac{2}{p_n}) = (-1)^{(p_n^2-1)/8} = 1$. Moreover, by the definition of the extended Jacobi-Legendre-Symbol, $(\frac{p_n}{2}) = +1$, hence

$$z'' \equiv 4\delta((+1)(+1)) \equiv 4 \cdot 0 \equiv 0 \mod 8$$

2nd case: $p_n = 8k \pm 3$, then

$$\frac{p_n^2-1}{8} = \frac{8^2k^2 \pm 2 \cdot 8 \cdot 3 \cdot k + 9 - 1}{8} = 2[4k^2 \pm 3k] + 1$$

is odd so that by Thm. 7, $(\frac{2}{p_n}) = (-1)^{(p_n^2-1)/8} = -1$. Moreover, by the definition of the extended Jacobi-Legendre-Symbol, $(\frac{p_n}{2}) = -1$, hence

$$z'' \equiv 4\delta((-1)(-1)) \equiv 4 \cdot 0 \equiv 0 \mod 8$$

This concludes the proof for a being a positive natural number. Now we come to the case where a is a negative number. The equation that we have to show varies slightly from the one we know already. By definition of the p-excess,

- $(-1)\text{–}\,\mathrm{excess}(Y) \equiv [(m-1)-1] - m \equiv -2$
- $2\text{–}\,\mathrm{excess}(Y) \equiv m - [-p_1 ... p_n + (m-1) + 4\Delta_2] \equiv (p_1 ... p_n) + 1 - 4\Delta_2$
- $p_j\text{–}\,\mathrm{excess}(Y) \equiv p_j + (m-1) + \Delta_{\backslash p_j} - m \equiv p_j - 1 + 4\Delta_{\backslash p_j}$
- $p\text{–}\,\mathrm{excess}(Y) \equiv n - n \equiv 0$ for all $p \notin Q$

Hence,

$$\sum_{p \in \overline{\mathbb{P}}} p\text{–}\,\mathrm{excess}(Y) \equiv \cancel{-1} - 1 + p_1 ... p_n + \cancel{1} - 4\Delta_2 + \sum_{j=1}^{n} (p_j + 4\Delta_{\backslash p_j}) - n$$

We have to show that this sum is congruent to 0 modulo 8 and since $-4 \equiv +4 \mod 8$, this is equivalent to saying that

$$4\Delta_2 + \sum_{j=1}^{n} 4\Delta_{\backslash p_j} \equiv -1 + (p_1 ... p_n) + \sum_{j=1}^{n} p_j - n \tag{0.12}$$

We will show this equation by induction on n.

The case $n = 1$ for equation (0.12) is again a straightforward computation. Let us proceed to higher dimensions:

$$
\begin{aligned}
\sum_{j=1}^{n} 4\Delta_{\backslash p_j} &\equiv \sum_{j=1}^{n-1} 4\delta\left(\frac{-p_1 ... p_{j-1}p_{j+1} ... p_{n-1}p_n}{p_j}\right) + 4\delta\left(\frac{-p_1 ... p_{n-1}}{p_n}\right) \\
&\equiv \sum_{j=1}^{n-1} 4\delta\left(\frac{-p_1 ... p_{j-1}p_{j+1} ... p_{n-1}}{p_j}\right) + \sum_{j=1}^{n-1} 4\delta\left(\frac{p_n}{p_j}\right) + 4\delta\left(\frac{-p_1 ... p_{n-1}}{p_n}\right) \\
&\overset{\text{ind. hyp.}}{\equiv} -1 + p_1 ... p_{n-1} + \sum_{j=1}^{n-1} p_j - (n-1) + \sum_{j=1}^{n-1} 4\delta\left(\frac{p_n}{p_j}\right) + 4\delta\left(\frac{-p_1 ... p_{n-1}}{p_n}\right) \\
&\equiv -1 + p_1 ... p_n + \sum_{j=1}^{n} p_j - n + p_1 ... p_{n-1} - p_1 ... p_n - p_n + 1 \\
&\quad + \sum_{j=1}^{n-1} 4\delta\left(\frac{p_n}{p_j}\right) + 4\delta\left(\frac{-p_1 ... p_{n-1}}{p_n}\right) \\
&\equiv -1 + p_1 ... p_n + \sum_{j=1}^{n} p_j - n + (1-p_n)(p_1 ... p_{n-1}) + (1-p_n) \\
&\quad + \sum_{j=1}^{n-1} 4\delta\left(\frac{p_n}{p_j}\right) + 4\delta\left(\frac{-p_1 ... p_{n-1}}{p_n}\right) \\
&\equiv \underbrace{-1 + p_1 ... p_n + \sum_{j=1}^{n} p_j - n}_{=\text{r.h.s!}} \\
&\quad + (-1)(p_n - 1)[p_1 ... p_{n-1} + 1] + \sum_{j=1}^{n-1} 4\delta\left(\frac{p_n}{p_j}\right) + 4\delta\left(\frac{-p_1 ... p_{n-1}}{p_n}\right)
\end{aligned}
$$

Put

$$\widetilde{z} := (-1)(p_n - 1)[p_1 ... p_{n-1} + 1] + \sum_{j=1}^{n-1} 4\delta\left(\frac{p_n}{p_j}\right) + 4\delta\left(\frac{-p_1 ... p_{n-1}}{p_n}\right)$$

then we have to show that $\widetilde{z} \equiv 0 \mod 8$. As in the computation for z in (0.8) we use quadratic reciprocity to obtain

$$\begin{aligned}
\widetilde{z} &\equiv (-1)(p_n-1)[p_1...p_{n-1}+1] + \sum_{j=1}^{n-1} 4\delta\left(\frac{p_n}{p_j}\right) + 4\delta\left(\frac{p_1...p_{n-1}}{p_n}\right) + 4\delta\left(\frac{-1}{p_n}\right) \\
&\equiv (-1)(p_n-1)[p_1...p_{n-1}-1+2] + \cancel{\sum_{j=1}^{n-1} 4\delta\left(\frac{p_j}{p_n}\right)} + \cancel{4\delta\left(\frac{p_1...p_{n-1}}{p_n}\right)} \\
&\quad + 4\delta\left((-1)^{\frac{p_n-1}{4}[(p_1-1)+...+(p_{n-1}-1)]}\right) + 4\delta\left(\frac{-1}{p_n}\right) \\
&\equiv \underbrace{(-1)(p_n-1)[p_1...p_{n-1}-1] + 4\delta\left((-1)^{\frac{p_n-1}{4}[(p_1-1)+...+(p_{n-1}-1)]}\right)}_{\equiv 0 \mod 8 \text{ by } (0.11)} \\
&\quad + 4\delta\left(\frac{-1}{p_n}\right) + 2(p_n-1) \\
&\equiv 4\delta\left(\frac{-1}{p_n}\right) - 2(p_n-1)
\end{aligned} \tag{0.13}$$

Now going through all the cases $p_n \in \{8k+1, 8k+3, 8k+5, 8k+7 \mid k \in \mathbb{N}\}$ yields the result. As an example we compute this for the case $p_n = 8k+3$: Here

$$\left(\frac{-1}{p_n}\right) = (-1)^{\frac{p_n-1}{2}} = (-1)^{4k-1} = -1$$

by Theorem 7 so that $4\delta(\frac{-1}{p_n}) \equiv 4 \mod 8$ but also $2(p_n-1) \equiv 2(3-1) \equiv 4$ so that $\widetilde{z} \equiv 4+4 \equiv 0 \mod 8$ and the rest of the cases works out in the same way. It remains to show (0.12) for a being even and negative. By following the above computation we see that $\widetilde{z}$ changes to $\widetilde{z} + \widetilde{z}'$ where $\widetilde{z}'$ is similar to the additional summand that we obtained in the case $a > 0$ and by another case-by-case analysis we also see that $\widetilde{z}' \equiv 0 \mod 8$. Hence we have seen that for every number $a \in \mathbb{Q}^{\times}$,

$$\sum_{p \in \overline{\mathbb{P}}} p\text{–excess}(Y) \equiv 0 \mod 8$$

which concludes the proof of the theorem. □

24 Corollary. *For every non-degenerate symmetric matrix $X \in \mathbb{Q}^{n \times n}$ the oddity formula holds, that is*

$$\mathrm{sig}_{-1}(M) + \sum_{p \geq 3} p\text{–excess}(M) \equiv \mathrm{oddity}(M) \mod 8$$

Proof. Let $X \sim_{\mathbb{Q}} \operatorname{diag}(a_1, ..., a_n)$ and put $Y := \operatorname{diag}(a_1...a_n, 1, ..., 1)$. Obviously, the oddity formula holds for X if and only if

$$\sum_{p \in \overline{\mathbb{P}}} p\text{-}\operatorname{excess}(X) \equiv 0 \mod 8$$

By (0.5), $\sum_{p \in \overline{\mathbb{P}}} p\text{-}\operatorname{excess}(X) \equiv \sum_{p \in \overline{\mathbb{P}}} p\text{-}\operatorname{excess}(Y)$ and by Theorem 22, $\sum\limits_{p \in \overline{\mathbb{P}}} p\text{-}\operatorname{excess}(Y) \equiv 0 \mod 8$. □

It is interesting to note that there is a second proof for the oddity formula that is completely different from what we have seen above. First note that it suffices to show the oddity formula for even matrices (that are matrices $X \in \mathbb{Q}^{n \times n}$ such that not only $X \in \mathbb{Z}^{n \times n}$ but also $x_{ii} \in 2\mathbb{Z}$) because if X is not even, then put d to be the least common multiple of all denominators that occur in X so that $X \sim_{\mathbb{Q}} 2dX2d = (2d)^2 X$ and $(2d)^2 X$ is even. The proof for even matrices is written down in [Str], Lemma 44. It needs the terms discriminant form and a Jordan decomposition of such (for a detailed treatment of these objects see [WeMSc]). In the version referred to, the proof contains a small mistake: In the notation of [Str], Lemmas 50, 51, 52 actually show that $g(J_q) = \sqrt{|J_q|}\gamma_p(J_q)$ for the indecomposable Jordan constituents but as $p\text{-}\operatorname{excess}(q^{\epsilon_1,1} \bigoplus q^{\epsilon_2,1}) = p\text{-}\operatorname{excess}(q^{\epsilon_1,1}) + p\text{-}\operatorname{excess}(q^{\epsilon_2,1})$ by definition (and analogously for the oddity), this property remains true for bigger Jordan blocks. In particular, for a fixed $p \in \mathbb{P}$, $\sum_{J_q \text{ is p-Jordan block}} p\text{-}\operatorname{excess}(J_q) \equiv p\text{-}\operatorname{excess}(D) \mod 8$ (and analogously for the oddity) so that

$$\begin{aligned}\sqrt{|D|}e_8(\operatorname{sig}(L)) = \sum_{\mu \in D} e^{Q(\mu)} &= \prod_{J_q} \sqrt{|J_q|}\gamma_p(J_q) \\ &= \sqrt{|D|}e_8\left(\operatorname{oddity}(D) + \sum_{p>2} p\text{-}\operatorname{excess}(D)\right)\end{aligned}$$

(note that since $D \cong J_1 \times J_2 \times ...$ where J_i are the Jordan blocks, $|D| = \prod_{J_q} |J_q|$) which is, in fact, the oddity formula.

References

[CS] John Conway, Neil Sloane, SPHERE PACKINGS, LATTICES AND GROUPS. Springer, 1988.

[Fi] Gerd Fischer, Lineare Algebra, Vieweg, 2005.

[Mil] John Milnor, Symmetric bilinear forms, Springer, 1973.

[Ca] John Cassels Rational Quadratic Forms, Dover Publications, 2008.

[Str] Fredrik Stroemberg, On the Weil representation for finite quadratic modules, http://www3.mathematik.tu-darmstadt.de/fileadmin/home/users/149/fqm_weil_representation_02.pdf

[Ne] Jürgen Neukirch, Algebraische zahlentheorie, http://www.springerlink.com/content/978-3-540-37547-0/

[WeMSc] Fabian Werner, Hecke Operators and the Weil representation. Masters thesis, 2011, http://happy-werner.de/uni/Mathe_MSc/mthesis.pdf.